Attachment 3: EPW Information Security As-a-Service Questionnaire

# Background

**This as-a-service questionnaire is necessary for the Department of <<Insert Department Name>> to complete its due diligence when departmental/government data in managed in third party provider systems/applications or is stored and used outside of the departmental network.**

It is specifically designed to elicit a high-level overview of the service being considered to refine and direct cyber security and information security questions prior to, or as part of, a procurement stage for a new system or a contract renewal stage for an existing system.

Responses provided may be used to inform any contractual arrangements entered with the department.

The questions included directly relate to the requirements contained within the Queensland Government’s [Information Security Policy (IS18:2018)](https://www.qgcio.qld.gov.au/documents/information-security-policy). Supplier’s responses will assist the Department to assess, mitigate and monitor information security risks associated with the offered solution.

For the purpose of this as-a-service questionnaire, a reference to “Service” or “Solution” means the ICT system/s the Supplier intends to use to capture, store and access Customer Data.

## Filling out this form

***This form is required only for Products / Goods / Services that include an ICT component.***

***Suppliers:***

* ***do not need to complete this form if the Offered Product / Goods / Service offering does not include an ICT component.***
* ***whose Product / Goods / Service offering includes only a minor ICT component, such as online ordering for your product/service offering, only respond to the questions that are relevant.***
* ***may be required to provide copies of certificates to support responses.***
* ***should leave a comment if they are unsure of any of the questions.***

# Supplier and solution details

| **Description** | **Required information** |
| --- | --- |
| Title describing the product or solution which includes the ICT component. | Name: |
| What service/s does the solution deliver? | Details: |
| Name of responding company / supplier. | Name:  ABN: |
| Date assessment completed. | Date: |
| Name, position, and company of person’s completing the form. | Details: |
| Is there an accountable person within the organisation who can attest to the security posture of the organisation based on independent or self-assurance activities and that information security risks are managed appropriately? This may include sharing of specific assurance information with clients. | Details: |
| Is there a data map/table available that includes field names, field descriptions and whether it is mandatory?  *Note: This will be used for Privacy Impact considerations.* | Choose an item.  If yes, please include/attach. |
| Are any third-party services or integrations used for the proposed solutions? | Choose an item.  If "Yes", who with:  Details: |
| Does the organisation of the solution/service have external information security governance arrangements for third party service level agreements, operational level agreements, hosting agreements or similar contracts to clearly articulate the level of security required and are regularly monitored? | Choose an item.  Please provide details: |
| Is security vetting (e.g. criminal history checks) undertaken for your employees and sub-contractors? | Choose an item.  If yes, provide details (including frequency): |
| Does the Supplier have a current insurance policy including claims for data breaches/loss? | Choose an item.  Details: |

# Hosting services and locations

| **Description** | **Required information** |
| --- | --- |
| Where is/would the solution/service components (live/back-ups/redundancy/testing/reporting) be hosted?  Select all that apply and provide details and location for each environment.  Please include details in the comments field if the data passes outside Australia (e.g., cognitive services in Azure) | ☐ On the EPW network  ☐ On the customer’s network  ☐ Private servers within Australia  ☐ Private servers outside of Australia  ☐ Third-party cloud service within Australia  ☐ Third-party cloud service outside of Australia  Name(s) of Third-party cloud service provider(s):  Cloud/Environment:  Hosting outside of Australia is located in:  Location:  Comments: |
| Is there any personally identifiable data contained within the solution/service (all environments) hosted offshore? | Choose an item.  Comments: |
| Where will your ICT support staff be accessing departmental data from? | ☐ No access to departmental data  ☐ Support accessing from within Australia.  ☐ Support accessing from outside Australia, located in: |
| Does the solution/platform include physical access controls to ensure only your authorised staff have access to the data? | Choose an item.  If yes, provide details: |
| Is data in the solution/service segregated from other customers’ data either virtually or physically? | Choose an item.  If yes, provide details: |
| Is production data in the solution/service segregated from non-production environments. | Choose an item.  If yes, provide details: |
| Does the solution/service provide data anonymisation / masking for environments depending on data classification/sensitivity with flexibility to adapt based on changing data sensitivity. | Choose an item.  If yes, provide details: |
| Is the solution’s data centre certified for ISO 27001/27002 compliance? | Choose an item.  If yes, provide evidence of certification.  Comments: |

# Security Measures

| **Description** | **Required information** |
| --- | --- |
| Does ensure your organisation ensure that your cloud infrastructure, operating systems and applications are regularly updated and kept at supported levels? | Choose an item. |
| Are operating systems and hardware regularly patched and at current patch levels?  Identify frequency of patching in comments. | ☐ Yes (if Yes, tick all that apply)  ☐ Computers (including network devices) with ‘extreme risk’ vulnerabilities are patched within 48 hours.  ☐ Computers use latest operating system versions.  ☐ Computers do not use unsupported OS versions.  ☐ No  Comments: |
| Is Patching applied to applications?  Select all that apply.  Identify frequency of patching in comments. | ☐ Yes  ☐ Workstation Applications (e.g., MS Office, Java, web browsers)  ☐ Server Applications (e.g., in-house developed apps, content management, webmail)  ☐ No  Comments: |
| What cryptographic protocols are utilised by this solution?  Select all that apply. | ☐ No cryptographic protocols are used.  ☐ The following cryptographic protocols are used:  ☐ Transport Layer Security (TLS) version:  ☐ Secure Shell (SSH) version:  ☐ Secure Multipurpose Internet Mail Extension (S/MIME) version:  ☐ Open PGP Message Format  ☐ Internet Protocol Security (IPSec).  ☐ Wi-Fi Protected Access 2 (WPA2)  ☐ Other:  Comments: |
| Has this solution/service disabled all TLS versions less than TLS 1.2 | Choose an item.  ☐ Minimum Transport Layer Security (TLS) version: |
| What encryption and hashing algorithms does the solution utilise to protect data at rest or in transit?  Select all that apply.  Reference: <https://www.qgcio.qld.gov.au/documents/data-encryption-standard>. | ☐ Data is not encrypted in transit.  ☐ Data is not encrypted at rest.  ☐ Data is encrypted at rest and/or in transit using:  ☐ 3DES (using 3 distinct keys)  ☐ AES128  ☐ AES192  ☐ AES256  ☐ RSA  ☐ SHA-2 (224)  ☐ SHA-2 (256)  ☐ SHA-2 (384)  ☐ SHA-2 (512)  ☐ Other:  Comments: |
| Is there a key management policy used within your organisation that facilitates a set of standards, procedures, and secure methods to safeguard the Confidentiality, Integrity and Availability of cryptographic keys? | Choose an item.  If yes, provide details: |
| Does the solution/service utilise consistent processes (deactivation, reactivation, expiry) and models (e.g. federation) for managing identities or any identities of users of the system (which may include Government employees or members of the public)? | Choose an item.  If yes, specify the processes and models: |
| Does the solution/service have the ability to implement SSO for authentication to the solution? | Choose an item.  Details: |
| Please provide details on account management processes (deactivation, reset, reactivation, expiry, review access levels) and models (e.g. federation) that are in place for managing identities. | Details: |
| Does the solution/platform include access controls to ensure only your authorised staff have access to the data? | Choose an item.  If yes, provide details: |
| Is each user within the Service/Solution required have a unique user ID and password (e.g. no shared accounts/passwords) | Choose an item.  Details: |
| Does the solution/service display a data privacy notification upon login and at various points of data access (particularly when accessing sensitive data). | Choose an item.  Details: |
| Do you regularly conduct reviews of user access levels? | Choose an item.  Details:  If yes, provide details: |
| If the solution/service requires the Customer to provide existing data, does the solution provide a secure method for uploading the data? Select all that apply. | ☐ No data is transferred/uploadable.  ☐ Data requires importing.  ☐ Direct upload by Customer  ☐ Direct transfer from other Customer solution  ☐ Provided by encrypted USB.  ☐ Provided by unencrypted USB.  ☐ Secure File Transfer Protocol (sFTP)  ☐ Other: |
| Are the following ASD Essential 8 strategies implemented for the solution/service?  References:   * <https://www.asd.gov.au/publications/protect/essential-eight-explained.htm> * <https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model>. | Are untrusted Microsoft Office macros disabled?  ☐ Yes ☐ No  Comments:  Are administration privileges restricted (vendor and application admins)?  ☐ Yes ☐ No  Comments:  Is application whitelisting in place?  ☐ Yes ☐ No  Comments:  Have you enacted user application hardening for relevant products (e.g. web browser, MS office, Powershell, PDF)?  ☐ Yes ☐ No  Comments:  Do you offer a multifactor authentication (MFA) service as a standard service?  ☐ No, MFA is not available  ☐ Yes MFA is available as standard:  ☐ Electronic (SMS, email, etc)  ☐ Physical token  ☐ Other: |
| How frequently do you conduct vulnerability assessments on the solution? | Choose an item.  If other, provide details: |
| What is the mean time to remediate any identified vulnerabilities?  Please provide details of your organisation’s treatment plan/approach for managing identified vulnerabilities. | ☐ critical vulnerabilities resolved within 3 days  ☐ critical vulnerabilities resolved within 4-14 days  ☐ critical vulnerabilities resolved in greater than 14 days  Details: |
| How frequently do you conduct full penetration testing or equivalent on the solution?  Please provide independent certification to confirm that Penetration Testing has been undertaken and that remediating actions for identified issues have been implemented. | Choose an item.  If other, provide details:  ☐ Redacted report provided.  ☐ Verification of pen test (or equivalent) provided |
| Have controls been implemented for the Open Web Application Security Project (OWASP) Top 10 security risks for web application services <https://owasp.org/www-project-top-ten/> | Choose an item.  Comments: |
| Please describe your approach to handling information security incidents including post-incident review process | Please describe process: |
| Does your solution’s audit logs provide the ability to audit access including following activities/attributes?  Select all that apply. | ☐ IP address  ☐ User account  ☐ Login attempts (successful/unsuccessful)  ☐ Activity performed (e.g. creation, modification, deletion)  ☐ Object activity was performed on (e.g. customer records)  ☐ access/view attempts to data elements marked as sensitive (e.g. private information, commercial in confidence).  ☐ change data history  ☐ date/time |
| Please provide your policy/process for notifying customers of any security breaches and/or data corruption/loss and actions to remediate? | Please describe policy/process: |
| Do you regularly review audit logs? | Choose an item.  Comments: |
| Do you allow the customer to review and export audit logs related to the use of the solution/service?  If "Yes" indicate the log types. | Choose an item.  If "Yes" indicate the log types: |
| What physical access controls are in place at the locations from which data may be stored? | ☐ None  ☐ Secure swipe card access  ☐ Biometrics  ☐ Coded access  ☐ Other, please detail: |
| Provide details of any other user access controls that are in place. | Detail: |
| Does the solution require minimum password details (e.g. 8 characters in length, number of character sets 3, frequency of change – min of 3 months) | Choose an item.  If yes, provide details: |
| Are passwords hashed, salted, and stretched before storing? | Choose an item.  If yes, provide details: |
| Please provide copy of the documented password policy for the solution/service | Choose an item.  If yes, provide details: |
| What are the password reset protocols? | Details: |

# Quality controls

| **Description** | **Required information** |
| --- | --- |
| Have change control processes been implemented to minimise disruption during business hours? | Choose an item.  Comments: |
| Does the solution have a Business Continuity Plan (BCP) in place? | Choose an item.  Comments: |
| What is the availability of the solution? | 24x7:      %  Business hours:      %  ☐ Negotiable: |
| Does the solution/service use data loss prevention (DLP) technologies? | ☐ Yes  ☐ No  If "Yes", indicate which technologies: |
| Is there a Recovery Time Objective (RTO) within the solution/service? | ☐ Yes  ☐ No  ☐ Negotiable  If Yes, indicate the timeframe:  If Negotiable, provide details: |
| Is there a Recovery Point Objective (RPO) within the solution/service? | ☐ Yes  ☐ No  ☐ Negotiable  If Yes, indicate the timeframe:  If Negotiable, provide details: |
| Is data made available to the customer in an agreed format, upon request? | ☐ No  ☐ Yes  ☐ Predefined:  ☐ Proprietary:  ☐ Other/agreed on request: |
| Are daily backups of data, software and configuration settings, stored disconnected, retained? | ☐ Yes  ☐ Retained for 3 months.  ☐ Restoration tested initially.  ☐ Restoration tested annually.  ☐ Restoration tested upon relevant infrastructure changes.  ☐ No daily backups  Comments: |
| How long is data retained for? This includes backups and archives. | Details: |
| Is data securely scrubbed and deleted on Customer request? This includes backups and archives. | ☐ Yes  ☐ No  Comments: |
| Is data deletion certified? | Choose an item.  Comments: |
| Do all employees of the organisation receive appropriate awareness education and training and regular updates on information security classification policies and procedures, their responsibilities, and principles, as relevant for their job function? | Choose an item.  Comments: |

# Compliance Controls

| **Description** | **Required information** |
| --- | --- |
| Is a systematic approach to managing information using an Information Security Management Systems currently in use or in the process of being implemented? | Choose an item.  Comments: |
| Is your organisation ISO/IEC 27001:2013 certified with the scope including all information, application and technology assets that form the solution/service?  If "Yes", supply the Certificate and Statement of Applicability (SOA). | ☐ No  ☐ Yes  ☐ Documentation provided.  ☐ Documentation not provided.  Comments: |
| Is the solution/service CSA Security, Trust & Assurance Registry (STAR) certified with the scope all information, application and technology assets that form the solution/service?  If "Yes", supply the Certification, Attestation and Consensus Assessments Initiative Questionnaire (CAIQ) v3.0.1. | ☐ No  ☐ Yes  ☐ Documentation provided.  ☐ Documentation not provided.  Comments: |
| If an IRAP assessment has been undertaken (Australian InfoSec Registered Assessors Program), to what level has the solution been certified? | ☐ Not IRAP assessed  ☐ IRAP assessed.  ☐ Unclassified DLM  ☐ Protected  ☐ Other: |
| If the solution processes electronic payments or holds credit card data, is it Payment Card Industry (PCI) Data Security Standards (DSS) compliant?  If "Yes", supply the Report on Compliance (ROC) and Attestations of Compliance (AOC). | ☐ Not Applicable – Solution does not process electronic payments.  ☐ No  ☐ Yes  ☐ Documentation provided.  ☐ Documentation not provided.  Comments: |
| Is an organisational wide risk management framework e.g., ISO 31000, in use and integrated with the Information Security Management Systems or planned to be? | Choose an item.  Comments: |
| Does your organisation have documented policies, procedures or controls for the items listed? | Revoking of access on staff (including Third Party Providers) exit: ☐ Yes ☐ No  Comments:  Use of personal devices by staff (including Third Party Providers): ☐ Yes ☐ No  Comments:  Secure development/coding, including reviews: ☐ Yes ☐ No  Comments: |
| Is personally identifiable information protected according to relevant privacy legislation and regulation where applicable, so all parties understand their obligations? | Choose an item.  Comments: |
| Confirmation of capability to provide a ASAE / ISAE 3402 Type 2 report as required for auditing purposes. | Confirmation of capability to provide a ASAE / ISAE 3402 Type 2 report:  ☐ Yes ☐ No  Comments: |

# References

* <https://www.asd.gov.au/publications/protect/essential-eight-explained.htm>
* <https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model>
* <https://www.qgcio.qld.gov.au/documents/data-encryption-standard>
* <https://www.qgcio.qld.gov.au/documents/information-security-classification-framework-qgiscf>
* <https://www.qgcio.qld.gov.au/documents/information-security-policy>
* <https://www.qgcio.qld.gov.au/documents/queensland-government-authentication-framework-qgaf>.

# Version Control

|  |  |
| --- | --- |
| **File Name** | DEPW Information Security As-a-Service Questionnaire |
| **Version** | 2.0 |
| **Last Modified** | 19/12/22 |